

FINAL  
DRAFT

INTERNATIONAL  
STANDARD

ISO/IEC  
FDIS  
27402

ISO/IEC JTC 1/SC 27

Secretariat: DIN

Voting begins on:  
2023-08-08

Voting terminates on:  
2023-10-03

---

---

## Cybersecurity — IoT security and privacy — Device baseline requirements

iTeh STANDARD PREVIEW  
(standards.iteh.ai)

[ISO/IEC FDIS 27402](https://standards.iteh.ai/catalog/standards/sist/3676e8ef-cc77-4b95-a177-918c93094761/iso-iec-fdis-27402)

<https://standards.iteh.ai/catalog/standards/sist/3676e8ef-cc77-4b95-a177-918c93094761/iso-iec-fdis-27402>

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.



Reference number  
ISO/IEC FDIS 27402:2023(E)

© ISO/IEC 2023

# iTeh STANDARD PREVIEW (standards.iteh.ai)

ISO/IEC FDIS 27402

<https://standards.iteh.ai/catalog/standards/sist/3676e8ef-cc77-4b95-a177-918c93094761/iso-iec-fdis-27402>



## **COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2023

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
CP 401 • Ch. de Blandonnet 8  
CH-1214 Vernier, Geneva  
Phone: +41 22 749 01 11  
Email: [copyright@iso.org](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

	Page
Foreword.....	iv
Introduction.....	v
<b>1 Scope.....</b>	<b>1</b>
<b>2 Normative references.....</b>	<b>1</b>
<b>3 Terms, definitions and abbreviated terms.....</b>	<b>1</b>
3.1 Terms and definitions.....	1
3.2 Abbreviated terms.....	3
<b>4 Overview.....</b>	<b>3</b>
<b>5 Requirements.....</b>	<b>4</b>
5.1 Requirements for IoT device policies and documentation.....	4
5.1.1 Risk management.....	4
5.1.2 Information disclosure.....	5
5.1.3 Vulnerability disclosure and handling processes.....	6
5.2 Requirements for IoT device capabilities and operations.....	6
5.2.1 General.....	6
5.2.2 Configuration.....	7
5.2.3 Software reset.....	7
5.2.4 User data removal.....	8
5.2.5 Protection of data.....	8
5.2.6 Interface access.....	10
5.2.7 Software and firmware updates.....	11
5.2.8 User Notifications.....	12
<b>Annex A (informative) Risk management guidance.....</b>	<b>13</b>
<b>Bibliography.....</b>	<b>15</b>

## Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see [www.iso.org/directives](http://www.iso.org/directives) or [www.iec.ch/members\\_experts/refdocs](http://www.iec.ch/members_experts/refdocs)).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at [www.iso.org/patents](http://www.iso.org/patents) and <https://patents.iec.ch>. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see [www.iso.org/iso/foreword.html](http://www.iso.org/iso/foreword.html). In the IEC, see [www.iec.ch/understanding-standards](http://www.iec.ch/understanding-standards).

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

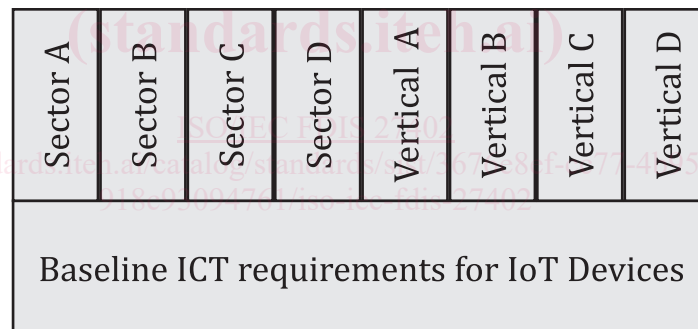
Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at [www.iso.org/members.html](http://www.iso.org/members.html) and [www.iec.ch/national-committees](http://www.iec.ch/national-committees).

## Introduction

With the increasing number of Internet of Things (IoT) devices and increasing reliance on such devices, the security and privacy risks relating to those “things” is expected to grow. Their widespread deployment in networks and systems make them easy and prime targets for cyber attacks.

This document provides a baseline set of information and communication technologies (ICT) requirements so that IoT devices are able to support security and privacy controls. A risk assessment is required to develop a risk treatment plan that identifies the necessary IoT device features and countermeasures. The management of systems which use IoT devices depends upon the capabilities of those devices (among other factors).

Broadly speaking, this document addresses ICT requirements for IoT devices that are made available to the market. The requirements in this document are intended as a baseline, upon which vertical markets (such as health, financial services, industrial, consumer electronics and transportation) can build additional requirements for the expected use and risks of IoT devices in their applications, as depicted in [Figure 1](#). In addition to this document, various sectors (e.g. private/industrial, public, defence, national security) and vertical markets have sector- or vertical-specific requirements, for example those found in ETSI EN 303 645<sup>[11]</sup> for consumer devices and the IEC 62443 series for industrial devices and systems. While this document can provide requirements for a conformity assessment scheme, it is expected that stakeholders for specific sectors and vertical markets will develop consensus around requirements specific to their contexts, building “on top” of this document. Subsequently, conformity assessment programmes can be developed around those specific sectors and vertical markets. This document would be effectively integrated into such programmes while providing a common set of baseline requirements.



NOTE Additional requirements may be developed or required by specific sectors and vertical markets.

**Figure 1 — Relationship between baseline requirements in this document and potential additional requirements**

As the complex technical landscape of IoT devices evolves, this document can support a scalable globally harmonized approach to the baseline security and privacy requirements and inform technical policy and regulatory initiatives.



# Cybersecurity — IoT security and privacy — Device baseline requirements

## 1 Scope

This document provides baseline ICT requirements for IoT devices to support security and privacy controls.

## 2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27400:2022, *Cybersecurity — IoT security and privacy — Guidelines*

ISO 31000:2018, *Risk management — Guidelines*

## 3 Terms, definitions and abbreviated terms

### 3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, ISO/IEC 27400, ISO 31000, and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

#### 3.1.1 identifier

information that unambiguously distinguishes one entity from another one in a given identity context

[SOURCE: ISO/IEC 23093-1:2022, 3.2.7]

#### 3.1.2 user interface

set of all components of an interactive system that provide information and controls for the user to accomplish specific tasks with the interactive system

[SOURCE: ISO 9241-110:2020, 3.10]

#### 3.1.3 internet of things IoT

infrastructure of interconnected entities, people, systems and information resources together with services which processes and reacts to information from the physical world and virtual world

[SOURCE: ISO/IEC 20924:2021, 3.2.4]

### 3.1.4

#### **IoT system**

system providing functionalities of *internet of things (IoT)* (3.1.3)

Note 1 to entry: An IoT system can include, but not limited to, *IoT devices* (3.1.5), *IoT gateways* (3.1.7), sensors, and actuators.

Note 2 to entry: Conventional IT devices such as smartphones and laptops can form part of an IoT system.

Note 3 to entry: IoT systems also include cloud and network connectivity.

[SOURCE: ISO/IEC 20924:2021, 3.2.9, modified — Notes 2 and 3 to entry have been added.]

### 3.1.5

#### **IoT device**

entity of an *internet of things (IoT) system* (3.1.4) that interacts and communicates with the physical world through sensing or actuating

Note 1 to entry: An IoT device can be a sensor or an actuator.

Note 2 to entry: An IoT device, in this context, is an assembled device usable for its intended IoT functions without relying on being embedded or integrated into any other product.

Note 3 to entry: IoT devices generally interact via communication interfaces.

[SOURCE: ISO/IEC 20924:2021, 3.2.6, modified — Notes 1, 2 and 3 to entry have been added.]

### 3.1.6

#### **IoT device developer**

entity that creates an assembled final *internet of things (IoT) device* (3.1.5)

Note 1 to entry: “Final” in this definition means the stage of delivery to the IoT service developer in the assemble process.

[SOURCE: ISO/IEC 27400:2022, 3.4]

### 3.1.7

#### **IoT gateway**

entity of an IoT system that connects one or more proximity networks and the IoT devices on those networks to each other and to one or more access networks

[SOURCE: ISO/IEC 20924:2021, 3.2.8]

### 3.1.8

#### **trusted computing base**

##### **TCB**

totality of protection mechanisms within a computer system, including hardware, firmware and software, the combination of which is responsible for enforcing a security policy

### 3.1.9

#### **cryptographic module**

set of hardware, software, and/or firmware that implements security functions and are contained within the cryptographic boundary

[SOURCE: ISO/IEC 19790:2012, 3.25]

### 3.1.10

#### **critical security parameter**

##### **CSP**

security-related information whose disclosure or modification can compromise the security of a *cryptographic module* (3.1.9)

Note 1 to entry: A CSP can be plaintext or encrypted.



Note 2 to entry: In the example, “certificates” refers to private keys matching public keys inside certificates.

EXAMPLE 1 Secret and private cryptographic keys, authentication data such as passwords, PINs, certificates or other trust anchors.

EXAMPLE 2 Configuration settings required for initialization.

[SOURCE: ISO/IEC 19790:2012, 3.18, modified — note 2 to entry and example 2 have been added.]

### 3.1.11

#### sensitive security parameter

#### SSP

*critical security parameters* (3.1.10) and public security parameters

[SOURCE: ISO/IEC 19790:2012, 3.110]

### 3.1.12

#### factory default

state of the device after factory reset or after final production/assembly

Note 1 to entry: This includes the physical device and software (including firmware) that is present on it after assembly.

### 3.1.13

#### fail-safe mode

device or feature which, in the event of failure, responds in a way that causes no harm, or minimizes the harm, to other devices, and causes no danger, or minimizes the danger, to personnel

[SOURCE: ISO 25197:2020, 3.32]

## 3.2 Abbreviated terms

API	application programming interface
ASLR	address space layout randomization
CPU	central processing unit
CSP	critical security parameter
ICT	information and communication technologies
IoT	internet of things
PIN	personal identification number
PSP	public security parameter
RoT	root of trust
TCB	trusted computing base
SWID	software identification
XML	extensible markup language

## 4 Overview

IoT systems bring security and privacy risks, and ISO/IEC 27400 provides general information and guidance about these risks and threats to security and privacy. To address these risks, users (organizations and consumers) should implement appropriate controls, which are also detailed in

ISO/IEC 27400. These controls cannot be implemented if the IoT devices do not have the supporting functionality (process policies, capabilities etc.)

The IoT system developers are expected to develop their own requirements and seek IoT devices that support them. This document provides baseline ICT requirements for IoT devices. In many cases, additional requirements will be imposed or are expected to address the security and privacy risks of specific vertical markets or higher risk environments.

## 5 Requirements

### 5.1 Requirements for IoT device policies and documentation

#### 5.1.1 Risk management

##### 5.1.1.1 Requirements

**5.1.1.1.1** IoT devices shall have documentation recording the results of a risk assessment process performed at the IoT device level in the context of a risk assessment at the system level.

**5.1.1.1.2** The risk assessment process shall take into account intended outcomes for the intended use case.

**5.1.1.1.3** The risk assessment process shall also take into account the needs and expectations of interested parties (e.g. those parties on networks to which the IoT device is connected), including physical and logical undesired effects.

NOTE 1 Risk assessment techniques can be found in IEC 31010 and ISO/IEC 27005.

NOTE 2 IoT device developers will usually perform the risk assessments and produce the risk treatment plans.

**5.1.1.1.4** The risk assessment shall take into account that IoT devices can be constrained (e.g. limited battery, little memory, 'weak' CPU), which informs the risk treatment process.

**5.1.1.1.5** Risk assessment and treatment processes shall be defined and applied as follows:

- a) determine if separate risk assessment and treatment processes are necessary for different products;
- b) select appropriate risk treatment options, taking account of the risk assessment results;

NOTE 1 Sector- or vertical market-specific standards can be used in addition to this document. Such a standard can provide a risk assessment and/or risk treatment plan specific to the sector or vertical market. Complying with such standards can be used to satisfy requirements in this document.

- c) determine all controls that are necessary to implement the risk treatment option(s) chosen;
- d) identify all security and privacy features of the IoT device from the controls identified in c) above;

NOTE 2 IoT device developers can design features as required or identify them from any appropriate source, such as an industry standard or sector guidance.

- e) compare the features identified in d) above with those in [5.2](#), and verify that no necessary features have been omitted;

NOTE 3 [5.2](#) contains a list of baseline features. Users of this document are directed to [5.2](#) to ensure that no requirements are overlooked.

NOTE 4 The features listed in 5.2 are not exhaustive and additional features and controls can be necessary based on specific vertical market segments or to address higher-risk use cases.

- f) produce a Statement of Applicability that contains the necessary features [see steps d) and e)] and justification for inclusions and the justification for exclusions of features from 5.2;
- g) if other standards related to device requirements are used, implement the requirements of those standards after steps a) through to f);
- h) formulate a risk treatment plan;
- i) inform the risk owner of the risk treatment plan and any residual risks, or where applicable, obtain their approval of the plan and acceptance of the residual risks.

**5.1.1.1.6** IoT devices shall implement the features and controls identified as necessary in its Statement of Applicability, as well as features and controls identified in 5.1.1.1.5, step g).

**5.1.1.1.7** The documentation shall be available for the supported lifetime of the product.

### 5.1.1.2 Additional recommendation(s)

The risk assessment and treatment processes should follow a widely-accepted method such as the one given in ISO 31000. For additional guidance on using ISO 31000, see Annex A.

### 5.1.1.3 Additional information

Interested parties, such as IoT device developers, system integrators, importers, retailers or regulatory bodies can perform such risk assessments.

IoT devices may contain security and privacy features and controls identified from any source such as sector- or vertical market-specific standards as well those defined in this document. IoT devices may contain additional controls other than those identified as necessary by the risk assessment.

## 5.1.2 Information disclosure

### 5.1.2.1 Requirements

**5.1.2.1.1** IoT devices shall have user documentation that lists the features that the IoT device provides to support controls for security and privacy, making it clear if any of the IoT device requirements in 5.2 are not included.

**5.1.2.1.2** Such information shall be publicly available for the period of time the IoT device is supported.

**5.1.2.1.3** IoT devices shall be covered by a security support policy and other supporting documentation wherein users are made aware in advance of when security updates will be discontinued.

### 5.1.2.2 Additional recommendation(s)

The requirements 5.1.2.1.1 to 5.1.2.1.3 should first be provided at the time of sale.

Guidance should be made available to the user post-purchase, possibly as part of the installation process, highlighting future IoT device events (such as updating software) and offering a means for the user to receive future communications.

The period of time when support is provided, as defined in the IoT device documentation, should be appropriate relative to the risks and to the expected lifetime of the product. Changing announced support periods should be avoided as doing so can disrupt the planning and operational cycles of users.